Sanction Guidelines for Privacy and Security Breaches

Media reports of healthcare privacy and security breaches are increasing, a trend that threatens efforts to build the consumer trust needed for health reform. The nature of these events has ranged widely from loss and theft of laptops and thumb drives to information leaks on Web sites to inappropriate staff access of celebrities' health records.

For privacy and security professionals following the news, the incidents reveal a wide span of provider philosophy and response regarding breaches. Facilities demonstrate varied degrees of access control management, differing stringency of enforcement policy, and inconsistent application of employee sanctions. Sanctions have ranged from gentle reminders to unspecified disciplinary action to termination of employment or contract.

Media reports have also shown unequal application of policies and sanctions within organizations. Rank-and-file employees have met with employment termination, and physicians have simply received counseling.[1] Organizations caught in the media headlights have shown varied readiness to address the press with a solid and serious message that embraces their privacy and security responsibilities.

Research demonstrates a humbling fact—the greatest threat to privacy and security rests within an organization's work force.[2] In an attempt to hold organizations accountable, federal and state laws have mandated breach prevention and penalties, and they are becoming more stringent.

While HIPAA's privacy and security rules establish a national floor for confidentiality, covered entities have been left to develop their own internal enforcement and sanctioning approaches.[3] Variation in the functionality of electronic health systems further increases the likelihood that organizations adopt disparate safeguard approaches.

Some states have passed legislation tightening privacy controls within their geographic area of influence, including private right of action, creating even wider gaps in national enforcement and sanctioning experiences.

This past patchwork of legislation and practice was met in 2009 with data breach provisions in the American Recovery and Reinvestment Act (ARRA).[4] Acting in tandem with HIPAA, the law's expanded and direct breach accountabilities at the individual and business associate levels place profound administrative responsibility on healthcare organizations and threaten life-changing enforcement on perpetrators—internal work force members, contractors, and external players alike.

Each organization has unique privacy and security programs deriving from particular cultural and operational constraints, yet all organizations face the same grand charge to uphold the confidentiality of

the health information they create and maintain.

To that end, this practice brief offers recommendations for the internal application of sanctions related to information privacy and security breaches for healthcare organizations that manage or service protected health information (PHI) or individually identifiable health information.

Because no two organizations are culturally or operationally alike, this practice brief is intended to bring awareness of the need for a united industry message of seriousness and responsibility toward the handling of breach events. It offers methods for sanction management within organizational policies.

This guidance mirrors the breach category approach now codified by ARRA, which encourages sanctions fitting to breach motivation, whether civil or criminal in nature.

Privacy and security professionals can have a direct impact on building consumer trust by showing a firm leadership commitment to consistent policy enforcement and sanction application for noncompliance.

Importance of Practice Standards for Breach Sanctions

The disparity in organizational response to employee malfeasance has a far-reaching impact on the healthcare industry. Consequences include the following.

Confusing message. An inconsistent organizational response to a breach sends a confusing message to both staff and the public. Healthcare workers moving from one organization to another find differing tolerance levels for enforcing the same directives.

Institutions have reported termination of some staff while issuing lesser reprimands or suspensions to other, higher-level staff for the same type of offense. Staff may interpret this to mean that it is acceptable to breach privacy or security rules as long as an individual holds a certain status in the organization. The industry should nurture an image of solidarity in enforcing PHI privacy and security.

Poor compliance. Staff in organizations with less stringent enforcement may weigh the level of risk to themselves against the potential advantages; for example, taking home PHI in order to catch up on work over the weekend. Staff that perceive lower risk will ignore security and privacy policies designed to protect PHI. Inequity in sanction application encourages poor compliance by individuals who know they will escape any serious consequence for breaching privacy and security policies.

Sanctions must be strong and prompt so that employees understand the organization is serious about information privacy and its enforcement.

Erosion of public trust. Public trust is eroded when significant variation is blatantly apparent in how healthcare organizations respond to a privacy or security breach both within and across entities and systems. The public must feel assured their personal health information has sufficient protections across the healthcare spectrum, particularly in this era of health information exchange.

Weakened position for dispute resolutions. Inequitable application of sanctions can affect the outcome of personnel actions at arbitration and grievance proceedings. Unequal penalties for similar offenses undermine the organization’s ability to prevail in dispute resolutions.

Vulnerability to lawsuits. The Centers for Medicare and Medicaid Services and the Office for Civil Rights are increasing their enforcement activities, and the federal judiciary is becoming engaged in enforcing HIPAA violations. The courts are just learning about HIPAA, and inconsistent application will affect how they view such issues.

Healthcare facilities leave themselves open to both individual and class action lawsuits when they do not have a strong, consistent enforcement program.

More regulation. Poor and inconsistent implementation of privacy and security safeguards invites further state and federal intervention. The California legislature recently enacted two privacy laws that impose more stringent reporting obligations and stiffer penalties on California facilities and individuals. Such laws place an additional administrative and financial burden on facilities. If the industry does not self-correct, then it leaves open the door to state and federal government intervention.

Questionable research. The validity of research may be called into question when privacy or security breaches are not handled consistently and expeditiously. Patients are less likely to participate in research studies with an organization that has an inconsistent sanction policy for privacy and security breaches.

It is in the best interest of the healthcare industry to address these issues in a proactive manner through development and agreement on sanction practice standards. Aside from the necessity to ensure patient privacy as an ethical obligation, it is smart business. Data breach notification laws in more than 40 states require an organization to notify breach victims, which can damage its reputation.[5]

Sanctioning Models

It is helpful to categorize sanctions according to the nature of the privacy or security incident for reporting purposes, trending, and corrective action determinations. Two models are depicted below.

Model 1—Categories of Privacy Incidents

In the first model, an organization creates categories defining the significance and impact of the privacy or security incident to help guide its corrective action and remediation steps:

- **Category 1:** Unintentional breach of privacy or security that may be caused by carelessness, lack of knowledge, or lack of judgment, such as a registration error that causes a patient billing statement to be mailed to the wrong guarantor.
- **Category 2a:** Deliberate unauthorized access to PHI without PHI disclosure. Examples: snoopers accessing confidential information of a VIP, coworker, or neighbor without legitimate business reason; failure to follow policy without legitimate reason, such as password sharing.
- **Category 2b:** Deliberate unauthorized disclosure of PHI or deliberate tampering with data without malice or personal gain. Examples: snooper access and redisclosure to the news media; unauthorized modification of an electronic document to expedite a process.
- **Category 3:** Deliberate unauthorized disclosure of PHI for malice or personal gain. Examples: selling information to the tabloids or stealing individually identifiable health information to open credit card accounts.

Sanctions may be modified based on mitigating factors. Factors may reflect greater damage caused by the breach and thus work against the offender and ultimately increase the penalty. Examples include:

- Multiple offenses
- Harm to the breach victim(s)
- Breach of specially protected information such as HIV-related, psychiatric, substance abuse, and genetic data
- High volume of people or data affected
- High exposure for the institution
- Large organizational expense incurred, such as breach notifications
- Hampering the investigation
- Negative influence of actions on others

Factors that could mitigate sanctioning could include:

- Breach occurred as a result of attempting to help a patient
- Victim(s) suffered no harm
- Offender voluntarily admitted the breach and cooperated with the investigation
- Offender showed remorse
- Action was taken under pressure from an individual in a position of authority
- Employee was inadequately trained

Model 2—Multifactor Model

In this model the organization takes corrective action and bases remediation on the highest level of category indicated. This model contains four major areas of risk: organization exposure, number of patients involved, purpose of action causing breach, and involvement of PHI that is covered by "special protections." If a breach falls into one or more risk areas on the chart, the corrective action is based on the highest category level of risk. For example, an error in the envelope-stuffing process for patient statements involving 1,000 patients would be a category 3 incident (see the table below).

From incident to incident, appropriate investigation and managerial discretion is necessary in declaring a misdeed. Organizations may find a sanctions determination document useful for ad-hoc sanctioning, as well as for comparative purposes and oversight trending. A sample document is included in this practice brief.

Categories of Personnel

An organization's sanctions policy and enforcement provisions must be broad enough to encompass all personnel, individuals, and business associates who have access to PHI created and maintained by the organization. The most common categories of personnel in a healthcare organization, including their related documents, are listed here, although this list should not be considered exhaustive.

Categories must likewise be adequately detailed to address different relationships and agreement or contract factors pertaining to respective work force and associate types. Included below are additional subcategories and areas that organizations may take into account when developing the sanctions policy.

- Employees, including bargaining unit employees (local unions of nonprofessional hospital staff and security and transport personnel and members of the American Nurses Association), such as possibly conflicting union contracts and nonbargaining unit employees, at-will employees,

contract workers

- Employed physicians
    - Human resources policies for physicians that may be different from those of the general employee population; contents of the medical staff bylaws, rules and regulations, due process
- Nonemployed medical staff
    - Contents of medical staff bylaws, rules, and regulations, including restrictions of clinical privileges or dismissal from the medical staff
- Academic appointments, including faculty appointments, due process, tenure
- Students
    - Student handbook
- Board members
- Volunteers, observers
- Third parties including business associates, business associate subcontractors, nonemployed individuals with access to information systems, billing companies, and any electronic data-sharing third parties
- Research agencies

Multifactor Model Categories

The multifactor sanctioning model identifies three categories of severity across four areas of risk. The organization takes corrective action and bases remediation on the highest level of category indicated. If a breach falls into one or more risk areas on the chart, the corrective action is based on the highest category level of risk.

Category	Exposure	Number Involved	Purpose	Special Protections
1	Low external exposure to organization	Involves a single patient	Ignorance or lack of education	No additional state or federal protections
2	Medium external exposure to organization	Involves 2–99 patients	Snooping or curiosity	Employees
3	High external exposure to organization	Involves 100+ patients	Malice, sale, or personal gain	HIV, mental health, adoption, etc.

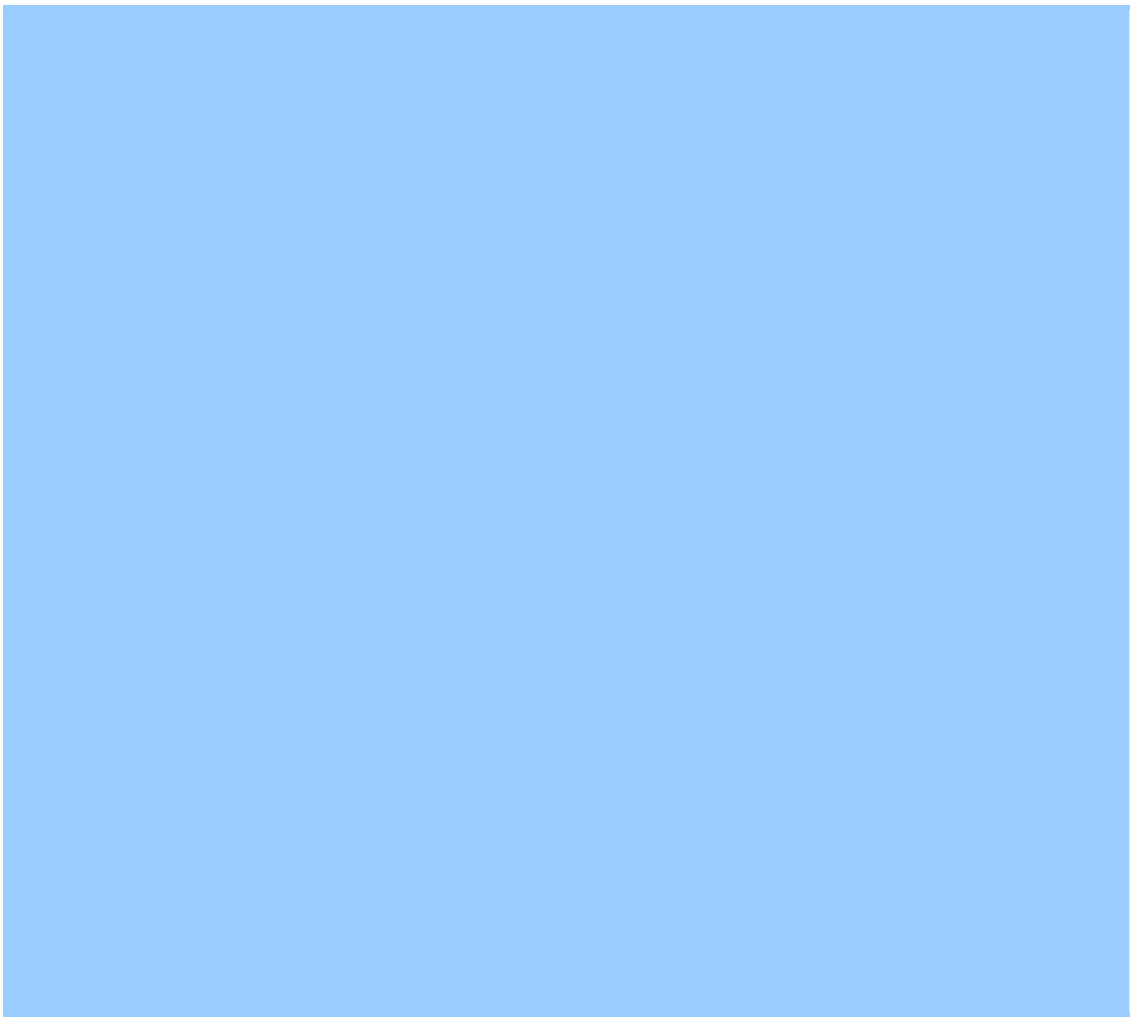
Breach Policy Recommendations

The HIPAA regulations require that imposed sanctions be consistent across the board irrespective of the status of the violator, with comparable discipline imposed for comparable violations. Organizational policy should address sanctions related to violations of both state and federal regulations as well as internal privacy and security policies. Organizations should enable application of general principles that will lead to fair and consistent outcomes:

1. To ensure a fair, consistent, and objective outcome, as many components of the policy as possible should be developed, documented, and approved by organizational leadership.
2. The policy should be written in a format that can accommodate ongoing updates to reflect modifications to the regulations and other institutional policies, including, but not limited to:
    1. Federal regulations (e.g., HIPAA, Family Educational Rights and Privacy Act, Red Flags Rule)
    2. State regulations (e.g., data breach notification laws, health codes)
3. The policy should be synchronized with other related institutional policies and contracts to ensure policies are blended together for a consistent message across the organization, including, but not limited to:
    1. Human resources policies and contracts
    2. Medical staff bylaws and rules and regulations
    3. Union contracts
4. The policy should be endorsed by all relevant departments, including legal, compliance, risk management, human resources, medical staff services, medical education, and the dean's office, as applicable.
5. Ideally the policy should be consistent across bargaining unit and nonbargaining unit entities as well as physician roles. If it cannot be, it should at least be internally consistent per contract and equivalent between groups, especially with regard to corrective action plans.
6. The policy should be subject to defined oversight with defined reporting responsibility. A possible model would include an ad-hoc sanctions committee that reports to the privacy and security committees, which in turn report to the compliance and oversight committee, and up to the audit and compliance committee of the board of trustees (see "Sample Reporting Structure" below).

Sample Reporting Structure

An organization's breach policies should be subject to defined oversight with defined reporting responsibility. One possible model includes an ad-hoc sanctions committee that reports to the privacy and security committees, which in turn report to the compliance and oversight committee, and up to the audit and compliance committee of the board of trustees.



Recommendations for Defining Key Terms and the Process

Organizations will benefit from clearly defining key terms and policy and procedure directives and expectations in their sanction policies. Clarity will enable consistent application across all departments and contracts. Consistency will strengthen relevant policies and prevent decisions from being overturned on appeal both internally and at administrative law hearings.

Organizations can address the following factors:

- Personnel categories
    - Employed medical staff
    - Voluntary medical staff
    - House staff
    - Board or trustee members
    - Volunteers
    - Students and job shadowers
    - Regional health information organization partners
    - Business associate employees
    - HIPAA-defined entities, including business associate and work force (see sidebar "HIPAA Definitions," below)
- Issues that affect breach categories
    - Unintentional, deliberate, malicious, personal gain

    - Incidental, accidental, inappropriate access
    - First infraction or repeated
    - Breach with harm or without harm
    - Scope of breach (e.g., number of patients, documents, files affected)
    - Adequacy of staff training
    - Adequacy of system protections and deterrents (policy and technical security)
    - Other exigencies
- Sanctions outcomes and how they may differ for employment relationship versus contracts
    - Documented conference with recommendations for additional, specific, documented training, if necessary
    - First written warning (and training, as above, if warranted)
    - Final warning, with or without suspension, with or without pay (training included, if warranted)
    - Severance of formal relationship: employment, contract, medical staff privileges, volunteer status
- The reporting structure
- Who is responsible for oversight

The sanctions process itself should be clearly defined, including:

- The decision-making body that will assess the incident and determine the level of sanction:
    - Membership by role and number of members
    - Permanency of the body
    - Definition of a quorum
    - Who appoints membership
- How outcome is decided: majority vote, plurality, or unanimity
- Process for appeals, if allowed:
    - Can a member of the committee hear an appeal?
    - Does the grievance process comply with contracts and bylaws?
    - Is there an appeal to senior management?
    - Guidelines such as time frames and information to be provided
- If there will be equivalency of sanction rather than consistency due to the nature of contractual obligations with entities, such as unions or the medical staff
- The role of credentialing as mandated by medical staff by law for both employed and voluntary medical staff and other credentialed practitioners (e.g., nurse practitioners, nurse midwives, nurse anesthetists, and physician assistants)

Audit and Reporting Process

Organizations should create mechanisms and assign responsibilities for evaluating sanctions over time to determine consistency and equivalency across roles by breaches, assess compliance with policies, and assess validity of policies.

Sanction data gathered for reporting purposes should include severity of sanction by type of infraction; severity of sanction by role; severity of sanction by bargaining unit status; and volume of sanctions applied relative to previous reporting periods and other institutions (if available).

The data should be reported to an interdisciplinary oversight committee that should include the chief privacy official, chief security official, and senior personnel representing a broad array of departments such as compliance, labor, legal, IT, administration, medical staff, risk management, finance, and internal

audit.

The data should be used to evaluate disciplinary patterns to ensure that comparable infractions result in comparable sanctions for all roles within the institution and across all entities within a multisite health system. Information should also be used to design corrective action for identified issues as well as anticipate and prevent identified risks. It can be communicated to the work force as a deterrent and used to justify sanctions at grievances and other labor hearings.

No two healthcare organizations will approach sanctioning and enforcement for privacy and security breaches in exactly the same way. Each healthcare organization needs to show a demonstrated, consistent ability to deal with privacy and security issues in its own way to ensure consumer trust. Inherent to privacy and security professional roles is a firm leadership commitment to consistent policy enforcement and sanction application for noncompliance.

HIPAA Definitions

Healthcare organizations developing breach policies and procedures should address personnel categories, which may require a review of HIPAA's definitions of business associates and work force.

A **business associate** is a person who:

- [on behalf of a covered entity (CE)]…but other than in the capacity of a member of the workforce of such CE (or arrangement), performs, or assists in the performance of a function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or
- provides, other than in the capacity of a member of the workforce of such CE, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such CE, where the provision of the service involves the disclosure of individually identifiable health information from such CE or from another business associate of such CE to the person.

Work force refers to employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

Notes

1. Ornstein, Charles. "Doctors Got off Lighter in UCLA Snooping Case." *Los Angeles Times,* April 12, 2008. Available online at http://articles.latimes.com/2008/apr/12/local/me-ucla12.
2. Krebs. Brian. "Report: Data Breaches Expose about 30M Records in '08." *Washington Post,* October 6, 2008. Available online at http://voices.washingtonpost.com/securityfix/2008/10/516_data_breaches_in_2008_expo.html.
3. HIPAA. Public law 104-191. Available online at http://aspe.hhs.gov/admnsimp/pl104191.htm.
4. American Recovery and Reinvestment Act of 2009. Public law 111-5. Available online at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f:h1enr.pdf.

5. State PIRG. “State PIRG Summary of State Security Freeze and Security Breach Notification Laws.” Available online at www.pirg.org/consumer/credit/statelaws.htm.

Resources

AHIMA 2007 Privacy and Security Practice Council. “How to React to a Security Incident.” *Journal of AHIMA* 79, no. 1 (Jan. 2008): 66–70.

Prepared by

Barbara Demster, MS, RHIA, CHCQM

Aviva Halpert, MA, RHIA, CHPS

Beth Hjort, RHIA, CHPS

Andrea Thomas-Lloyd, MBA, RHIA, CHPS

Acknowledgments

AHIMA 2008 Privacy and Security Practice Council

AHIMA 2009 Privacy and Security Practice Council

The information contained in this practice brief reflects the consensus opinion of the the professionals who developed it. It has not been validated through scientific research.

Article citation:
AHIMA. "Sanction Guidelines for Privacy and Security Breaches" *Journal of AHIMA* 80, no.5 (May 2009): 57-62.